

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF VIRGINIA  
CHARLOTTESVILLE DIVISION

IN THE MATTER OF THE SEARCH OF:  
**202B Tiffany Dr.**  
**Waynesboro, VA 22980**

Case No. 5:19-mj-00038

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, William Ury, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for 202B Tiffany Dr., Waynesboro, VA 22980 (PREMISES) for evidence stored at the premises controlled by William Eugene Angus UNDERWOOD. The articles to be searched for are described in the following paragraphs and in Attachment A.

2. I am a Special Agent with the United States Capitol Police (USCP), and have been since August 2018. I am currently assigned to the USCP Investigations Division, Threat Assessment Section. Prior to working in the Investigations Division, I was a uniformed officer with the USCP from April 2003 to August 2018. Prior to employment with the USCP, I was a Deputy Sheriff in Union County, Illinois from November 1990 to February 2003. I am a graduate of the Criminal Investigator Training Program at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. In the course of my employment as a Special Agent with the USCP, I have received training regarding the application for and execution of arrest warrants. In my current assignment, I have participated in and conducted investigations involving illegal activity, including threatening communications, both locally and interstate.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of Title 18 U.S.C. § 875(c) may be at the subject address, and there is probable cause that those violations may have been committed by William Eugene Angus UNDERWOOD (UNDERWOOD).<sup>1</sup> There is also probable cause to search the information described in Attachment A for evidence of these crimes, as further described in Attachment B.

### **PROBABLE CAUSE**

1. A check of UNDERWOOD's Virginia driver's license reflects an address of 202B Tiffany Dr. Waynesboro, VA 22980-3243.

2. On August 14, 2019, the United States Capitol Police - Investigations Division-Threat Assessment Section received information reported by Cooperating Witness 1 (CW-1).

3. CW-1 reported he was communicating with UNDERWOOD via Facebook Messenger on the night of August 12, 2019 and again on August 13, 2019.

4. CW-1 reported UNDERWOOD was expressing mental and emotional issues he was experiencing with his vehicle and with his girlfriend on the night of August 12, 2019 (Exhibit A, Pages 1-4).

5. CW-1 reported UNDERWOOD followed with the conversation with the following statement: "And to top it off, the US is going down the shitter faster than I wanted it

---

<sup>1</sup> Title 18, United States Code Section 875(c) prohibits the transmission, in interstate commerce, of true threats to kidnap and/or injure another individual – such as, e.g., an interstate telephone call.

to, and I'm having legitimate serious thoughts about getting a plate carrier and rifle, and going off on my own kind of spree in the capital building.”<sup>2</sup>

6. When CW-1 asked what good such action would do, UNDERWOOD stated: “It would make me feel better. And frankly, that particular action is better than inaction. Go all founding father on their asses, clean slate this shit. I keep reading the manifestos of all these shooters, and I legitimately understand why they do what they do. I think their targets are fucked up, but their reasons check out with me. Gotta head back to the floor now man. Just thought I'd give you a quick run down.”<sup>3</sup>

7. The pathway to violence is generally comprised of the following steps: grievances, violent ideation, research and planning, pre-attack preparation, probing and breaching, and committing violence. Although not all documented lone wolf attacks precisely follow this template, there are many consistencies along the path. Where one shooter may skip one step, others may retreat back before continuing on. Two examples follow:

- The events of March 15, 2019 in Christchurch, New Zealand, and the manifesto that was published by the actor allow investigators to follow along the actor's pathway to violence. The actor in Christchurch discussed over many pages his grievances with his government, discussed how the “extermination of the white race” could be stopped, discussed at length why he chose the firearms he did, to include a discussion of why he chose certain ones over the other. This particular actor all but skipped pre-attack planning, narrowing his intended targets down to three with no set goal of where and when to start his attack. Ultimately, with no intervention the attack was committed by an actor with no military background yielding the deaths of 51 souls.
- The events of August 4, 2019 in Dayton, OH demonstrate that the pathway to violence is different for each actor. In this case the actor did not leave a manifesto for investigators

---

<sup>2</sup> Exhibit A (A series of Facebook screen captures and photos provided by CW-1 to law enforcement.)

<sup>3</sup> Exhibit A at 2.



to follow, however there were other clues that went unnoticed until after the attack. The Dayton actor expressed interest in violence as a means to solve his perceived issues. Through the months prior to the shooting it was discovered that his rhetoric and internet searches became more violent and promoted the idea that violence would ultimately be the answer. It is believed that this actor was inspired by the manifesto left by the actor of the El Paso shooting.

8. From Exhibit A, the following facts can be gleaned: UNDERWOOD'S personal life has begun to fracture (issues with girlfriend, emotional issues)(Exhibit A at 1); UNDERWOOD stated he is "having serious thoughts about getting a plate carrier and rifle, and going off on my own kind of spree in the capital [sic] building" (Exhibit A at 1); he is reading the manifestos of other actors and identifying with them (Exhibit A at 2), and he is researching weapons, alcohol, and armor (Exhibit A - google search history).

9. CW-1 communicated to UNDERWOOD that violence was not the answer, and UNDERWOOD replied: "Bro, our freedoms are already gone. We have no power other than violence."<sup>4</sup>

10. CW-1 questioned UNDERWOOD about his future legacy and told UNDERWOOD he had so much to live for. UNDERWOOD communicates "That's exactly my point. Facebook is collecting it all. It's all monitored. And I'll probably get my door kicked in soon. For having treasonous thoughts and conversations. Fuck my rights, yeah? I'd leave the legacy of a free man. Realistically, no, I'm not going to do anything, because it would ultimately serve no purpose. But I'd really like to buy a cabin in Northern Montana, and just fucking disappear. The fact that we can't even discuss such a thing as this without being a crime though, tells me all I need to know about my rights and freedoms. They're only given to me by violence of keeping them. If we cannot have faith in our government or process, then how else are we

---

<sup>4</sup> Exhibit A at 2.

expected to change things? All of these epiphanies and questions led me to saying what I've said. Do you see where I'm coming from? The only options are to fight or run. Lol this is why I don't open up a lot."<sup>5</sup>

11. CW-1 communicated that "murdering people in cold blood won't do shit." And UNDERWOOD replied: "What will do shit? Also, like 50 revolutions say your wrong."<sup>6</sup>

12. CW-1 communicates that mass protest is the answer and loose actions will not do the country good in which UNDERWOOD replies: "Nah, not a loose action. A revolution. And when the fuck has protest accomplished anything? I'd love an example."<sup>7</sup>

13. CW-1 communicates he cannot morally condone UNDERWOOD's statements, to which UNDERWOOD replied: "But you can morally condone letting the government trample all over its own people."<sup>8</sup>

14. The communication provided to law enforcement ends with CW-1 giving his opinion of the state of the nation to come, and receives no reply from UNDERWOOD.<sup>9</sup>

15. CW-1 also informed law enforcement that, on the evening of August 13, 2019 (the day after the communications set forth above), he received another Facebook message from UNDERWOOD, which showed a list of items for which UNDERWOOD had recently searched

---

<sup>5</sup> Exhibit A at 3.

<sup>6</sup> Exhibit A at 4.

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

online.<sup>10</sup> The list of items for which UNDERWOOD had searched included Glock 17 price, bottle of jack, Waynesboro to Emporia, VA, and level 5 ballistic plates.<sup>11</sup>

16. UNDERWOOD followed the list with the statement: “Lol I think my FBI agent is on high alert” “Bottle of jack, level 5 plates, glock, and the drive from my place to a DC suburb Imao”.<sup>12</sup>

17. UNDERWOOD communicated to CW-1 that he has a friend who lives in DC and was planning to visit. CW-1 replied the statements scared him for a second, to which UNDERWOOD replied: “So imagine how my agent feels.”<sup>13</sup>

18. CW-1 reported UNDERWOODS’s Facebook address as: [www.facebook.com/sameasiteverends](https://www.facebook.com/sameasiteverends)

19. CW-1 reported UNDERWOOD goes by the name Eugene.

20. Agents submitted to Facebook an emergency request for subscriber information and IP session logs for the user name: [www.facebook.com/sameasiteverends](https://www.facebook.com/sameasiteverends). A review of the information provided by Facebook in response revealed that the subscriber’s name is Eugene UNDERWOOD, with phone number 540-480-7138.

21. Agents performed database searches associated with phone number 540-480-7138, and the results confirmed an association with William UNDERWOOD of Staunton, VA.

---

<sup>10</sup> Exhibit A at 5-6.

<sup>11</sup> *Id.*

<sup>12</sup> Exhibit A at 5.

<sup>13</sup> *Id.*

22. Facebook also provided to law enforcement IP session logs that showed IP address 2601:05ce:0300:4514:490e:14d1:bfd2:4aa4 was being used on 2019-08-13 at 22:03:41 UTC, by a Facebook account registered to UNDERWOOD.<sup>14</sup>

23. An open source search of the IP address 2601:05ce:0300:4514:490e:14d1:bfd2:4aa4 revealed the provider as Comcast.

24. Agents submitted an exigent request to the Comcast Legal Response Center for subscriber information associated with the IP address 2601:05ce:0300:4514:490e:14d1:bfd2:4aa4 and was provided with the following subscriber information: William UNDERWOOD of 202B Tiffany Dr. Waynesboro, VA 22980, phone number of 540-480-7138.

25. Law enforcement database checks on UNDERWOOD provided a date of birth in the year 1995, and a social security number XXX-XX-5002.

26. CW-1 provided photos of a vehicle to law enforcement, bearing Virginia license plate ROKKET. Law enforcement conducted database checks on Virginia registration ROKKET and learned the registered owner was William Eugene Angus UNDERWOOD, of 202B Tiffany Drive in Waynesboro, Virginia 22980-3243. Law enforcement surveillance on August 15, 2019 revealed the vehicle was parked in front of 202B Tiffany Drive in Waynesboro, Virginia, the suspected residence of UNDERWOOD.

#### **USE OF COMPUTERS AND CELLULAR PHONES IN THREAT RELATED OFFENSES**

27. Based on affiant's training and experience and discussions with other law enforcement officers, persons committing or intending to commit threat related offenses often

---

<sup>14</sup> Communications at Exhibit A at 5.



utilize computers, data storage devices (e.g., external storage devices, ZIP disks, and CD-Roms), and other electronic communications equipment , including cellular telephones. These persons often use computers, cell phones, and peripheral devices to search the internet and to communicate and transmit threats to recipients of threat related activities.

### **TECHNICAL TERMS**

28. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.
- b. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.



- c. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- d. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- e. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- f. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- h. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash

memory, CD-ROMs, and other magnetic or optical media.

**COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

29. As described above and in Attachment B, this application seeks permission to search for records and other items that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

30. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap"



or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.



- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

32. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained

above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

34. If it is found that at least two people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those

computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

### **AUTHORIZATION REQUEST**


35. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41.

36. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until execution of the search warrant. These documents discuss an ongoing criminal investigation that is neither public nor known to the subject of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving the subject an opportunity to destroy or tamper with evidence, endanger the safety of investigators, change patterns of behavior, notify confederates, and flee from prosecution.

### **OATH**

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

  
\_\_\_\_\_  
William Ury, Special Agent  
United States Capitol Police

Received by reliable electronic means and sworn and attested to by telephone on  
this 15 day of August 2019.

*Robert S. Ballou*  
\_\_\_\_\_  
ROBERT S. BALLOU  
UNITED STATES MAGISTRATE JUDGE